Access Grid User's Guide

version v16 – January 2008

Table of Contents

Introduction.....5
Hardware Requirements.....6
Computers.....6
Network.....6
Display.....7
Cameras.....7
Microphone Headset.....7
Installing the AccessGrid Toolkit (AGTk).....8
Special Note on AccessGrid Versions.....8
Software Installation - Windows.....8
Upgrading the AGTk – Windows.....9
Software Installation – Linux.....10
Upgrading the AGTk – Linux.....11
Running the VenueClient.....12
Creating a Profile.....12
Connecting to the VenueServer.....12
Checking Multicast Connectivity - Using the Multicast/Unicast Bridge.....13
Adding Video Capture Capability.....14
Basic Video (VIC) Operation.....14
Basic Audio (RAT) Operation 15
VenueServer Navigation.....15
Node Management – Services and ServiceManagers.....16
AudioService.....16
VideoService.....16
VideoConsumer.....16
VideoProducer.....17
Viewing and Managing Services and ServiceManagers.....17
Adding a ServiceManager.....17
Adding a Service to a ServiceManager.....18
Saving Your Configuration.....18
Certificate Management.....19
Importing Certificates.....20
Exporting Certificates.....20

Requesting A New Certificate.....21
Viewing/Importing Pending Requests.....21
Using Grid Canada Certificates.....22
Creating A Globus Proxy.....23
Additional Resources.....24
Links.....24
WestGrid Access Grid Documentation.....24
Access Grid Documentation.....24
The Access Grid Documentation Project.....24
Vic User Guide.....24
AccessGrid Mailing Lists.....24
Troubleshooting.....25
Network.....25
Video.....25
Reception Greyed Out.....25
No Feeds Received.....25
Vic Crashes.....25
Selecting a Video Source.....25
Audio.....26
Reception.....26
Transmission.....26
Contact.....27

Illustration Index

Illustration 1: Access Grid Download Page....8
Illustration 2: Node Profile....12
Illustration 3: VenueClient....13
Illustration 4: Vic Main Window....14
Illustration 5: Vic Single Video Window....14
Illustration 6: Vic Options 14
Illustration 7: RAT Main Window....15
Illustration 8: Node Management Window....17
Illustration 9: Add ServiceManager Dialog....17
Illustration 10: Add Service Select....18
Illustration 11: Store Configuration Dialog....18
Illustration 12: Import Identity Certificate....20
Illustration 13: Successful Certificate Import....20
Illustration 14: Exporting Identity Certificates....20
Illustration 15: Certificate Request Status....21
Illustration 16: Successful Certificate Import....22
Illustration 17: Creating a Globus Proxy....23
Illustration 18: Windows Recording Select....27
Illustration 19: Windows Recording Volume Control....27

Introduction

The Access Grid (AG) is a collaboration technology which offers a unique and high-quality experience for users and participants of collaborations. It is described on the Access Grid website (www.accessgrid.org) as “an ensemble of resources including multimedia large-format displays, presentation and interactive environments, and interfaces to Grid middleware and to visualization environments.” AG technology is now used at over 237 sites, across 25 different countries for activities such as very large distributed meeting, lectures, seminars, and other interactive collaborative tasks.

Typically, an AG ‘node’ consists of one or more computers, a high-end echo cancellation unit, multiple large displays, and multiple camera and microphone inputs – all housed within a large conference style room. An 'Access Grid Station’ (more commonly referred to as a 'Personal Interface to the Access Grid' or PIG node), by contrast, is a single computer with the ability to access and make use of the AG and its related services.

This document will guide you through the download, install and basic troubleshooting of setting up a personal AG node.

This manual is set up to be as simple and easy to follow as possible. To accomplish this, the following icons will be used to indicate special areas that may be of interest to you.

Indicates that a user action is required to accomplish a task

Indicates the computer’s response

Indicates a hint, tip or general information

Indicates a warning

Hardware Requirements

Due to the nature of collaboration using AG (multiple video feeds from many sites), it is important to have a fairly powerful computer with a good network connection to fully utilize the AG. However, since this document is primarily targeted at those users wishing to determine if their current computer is adequate for participating in AG meetings, this document will not serve as a hardware specification but as a recommendation of system capabilities that are required. We provide suggestions below that will guide new users of the AG in determining if their current technology is adequate and if not what hardware upgrades they might require to make practical use of the AG. For those AG users that are building a new system, sending an email to support@westgrid.ca would be a good place to start.

Computers

In general, any modern computer system should be adequate for an Access Grid node. Due to the amount of video encoding/decoding that takes place during collaboration, the amount of memory should be maximized. Although not necessary, it is useful to invest in slightly higher quality video and audio cards than generic or 'on-board' devices. By using the widely used nVidia, ATI or Matrox video cards and standard SoundBlaster audio cards, hardware related issues can usually be avoided.

Network

Due to the amount of data (video, audio, application data) that is distributed during a typical AG collaboration, the quality of the network connection is very important. Both bandwidth and latency are important factors. Users communicating via AG over the University research network (the WestGrid network, the regional research networks, and the national research network) should not have any issues with performance. If communicating over the generic Internet, quality and performance of the audio and video will vary depending on the quality of network connection. Small meetings (two or three sites with a small number of video feeds) can be effectively held with users using high-speed home networks (ADSL, cable) if the home network connection is not loaded with other traffic. Quality and performance can vary drastically in these instances.

In addition to raw performance of the network connectivity, the AG technology uses IP Multicast to facilitate the multi-site nature of collaboration. Multicast provides network efficiency by allowing the network infrastructure to optimize the traffic for many sites without requiring complex Multipoint Control Units (MCUs). Depending on your location and service provider, multicast may or may not be enabled. While some universities and research facilities offer full multicast enabled network access, most typical commercial Internet Service Providers (ISP's) do NOT support multicast traffic. The WestGrid and Canarie backbone networks are multicast enabled, but many University routers are not. Check with your network administrator to confirm whether your network is multicast enabled.

If multicast is not available on your local network, WestGrid offers multicast to unicast bridging capabilities for WestGrid users. For operation using a multicast bridge see the “Using The Multicast/Unicast Bridge” section below.

Display

As noted, collaborations typically involve many sites – each with multiple video feeds. In addition, shared applications or visualizations are often the topic of the collaboration. This can raise ‘screen real-estate’ problems if you are using a small display. By investing in a large display – or a multi-headed display adaptor with multiple monitors, this problem can be minimized.

Cameras

For a typical Access Grid Station set up, any usb cam will be sufficient. Again, as above, the more you invest, the higher the quality output. This is especially true of webcam.

If you would like to have higher quality video capture, you can invest in a 'video capture card' (such as a Hauppauge) and use a DV camera as input.

Microphone Headset

It is strongly recommended that a good quality headphone/microphone headset be purchased to maximize the quality of the collaboration. If a standard microphone and desktop speakers are used, the audio from the speakers will be picked up by the microphone and be sent back to the other sites as echo. You will not be able to hear this echo; however, it is very distracting for the other sites and can destroy the quality of the collaboration. For single person Grid Stations, it is recommended that each user use a headset and microphone rather than desktop speakers. Also, it is useful to have both a volume control and a mute button on the headset or the audio cable.

Installing the AccessGrid Toolkit (AGTk)

Now that you have the hardware, its time to set up the AccessGrid software to run on your system.

Special Note on AccessGrid Versions

There are numerous past versions AccessGrid available. Specifically, AG2.4 (released in 2005) is still currently available; however, is not compatible with the latest AG3 releases. Within WestGrid, our infrastructure is based on the AG3 versions. While we still have some AG2.4 based services available, these services will be phased out. It is recommended that all users switch to AG3.1 For more information on versions, please contact support@westgrid.ca.

Software Installation - Windows

Installation of the Access Grid software on Windows is similar to installing any other piece of software under the Windows operating system. However there is some prerequisite software that is required to make the AG software operate, namely Python and wxPython.

All of the software and prerequisites can be found by following the 'software' link at the main AccessGrid page located at: http://www.accessgrid.org/

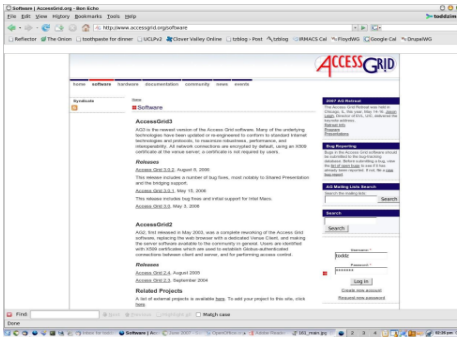

Illustration 1: Access Grid Download Page

To install AGTk on Windows:

1. **Navigate to the main Windows AccessGrid download page by following the 'Software' link at http://www.accessgrid.org/software**
2. **Select the AccessGrid 3.1 release link**
3. **Select the Windows XP link**

4. **Download and install the prerequisite Python, wxPython and Bonjour software from the link on the AGTk download page.**
5. **Download and Install the AccessGrid Toolkit**

Once the software is installed – please see the section called 'Running the VenueClient' below.

Upgrading the AGTk – Windows

We have found that often it is better to completely uninstall and delete your configuration directories before installing a newer version of AGTk. Since it usually isn't that difficult to reconfigure once its upgraded (setting up the service managers etc), it is well worth the effort since it usually saves you from many odd problems that can be extremely difficult to debug.

Before Upgrading your AGTk:

1. **Export any personal certificates to a known, safe locations. (Preferences - > Certificate Manager in the VenueClient) This step is only required if you are using personal certificates – not anonymous certificates which are used in default situations.**
2. **Uninstall AGTk, Python & wxPython from the Control Panel -> Add/Remove Programs**
3. **Delete the \Documents and Settings\All Users\Application Data\AccessGrid directory**
4. **Delete the \Documents and Settings\<username>\Application Data\AccessGrid directory from all users that use AG on that machine.**
5. **Reinstall Python, wxPython and AGTk as described in the previous section.**

Most default installations use anonymous certificates; however if you are using personal WestGrid certificates as identification in AccessGrid, it is important that you backup your existing certificates to a safe and known location before deleting any configuration directories. . To do this, start your venue client and choose "Preferences -> Manage Certificates -> Export". See the "Exporting Certificates" section below for more details.

Software Installation – Linux

There are many different Linux distributions capable of running the AccessGrid software – each with unique installation instructions. Since very detailed and easy instructions already exist for installing AccessGrid on these platforms , this section will only provide links to this external documentation.

Installation guides for Fedora can be found at:

http://www.accessgrid.org/documentation

For other distibutions, please search www.accessgrid.org or contact support@westgrid.ca

Once the software is installed – please see the section called 'Running the VenueClient' below.

Upgrading the AGTk – Linux

We have found that often it is better to completely uninstall and delete your configuration directories before installing a newer version of AGTk. Since it usually isn't that difficult to reconfigure once its upgraded (setting up the service managers etc), it is well worth the effort since it usually saves you from many odd problems that can be extremely difficult to debug.

Before Upgrading your AGTk:

1. **Export any personal certificates to a known, safe locations. (Preferences - > Certificate Manager in the VenueClient)**
2. **Uninstall AGTk (platform dependent)**
3. **Delete the /etc/AccessGrid directory**
4. **Delete the ~/.AccessGrid directory from all users that use AG on that machine.**
5. **Reinstall AGTk as described in the previous section.**

Most default installations use anonymous certificates; however if you are using personal WestGrid certificates as identification in AccessGrid, it is important that you backup your existing certificates to a safe and known location before deleting any configuration directories. . To do this, start your venue client and choose "Preferences -> Manage Certificates -> Export". See the "Exporting Certificates" section below for more details.

Running the VenueClient

To start the VenueClient:

1. **Click on the VenueClient shortcut created during installation**
   OR From the command line – run: "VenueClient.py –personalNode"

Creating a Profile

When launching the AccessGrid software for the first time, a 'Node Profile' information page will appear.

To create a profile:

1. **Fill in the appropriate information for Name, Email, Phone Number, Location and Support Information.**
2. **Set your home venue to the Main WestGrid VenueServer at:**

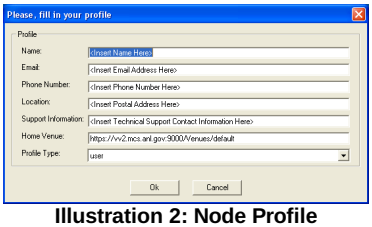

Illustration 2: Node Profile

https://venueserver.westgrid.ca:8000/Venues/default

3. **Set the appropriate Profile Type – User (single person node) or a Node (Full Room Configuration)**

At this point the VenueClient should appear. Before completing the VenueClient configuration, the user certificates must be properly imported into the VenueClient.

Connecting to the VenueServer

Once installation is complete, starting your Access Grid Station is as simple as choosing the VenueClient shortcut or by running 'VenueClient –personalNode' from the command line.

Once the VenueClient is started, the main VenueClient window will appear. The next step is to connect to a VenueServer and begin collaborating.

To connect to a VenueServer:

1. **Enter a VenueServer url into the address bar**
2. **Press the 'GO' button**

The main WestGrid VenueServer is located at
https://venueserver.westgrid.ca:8000/Venues/default

Once connected, the VenueClient will show the current status. Here is a basic layout of the VenueClient in the WestGrid Server Lobby

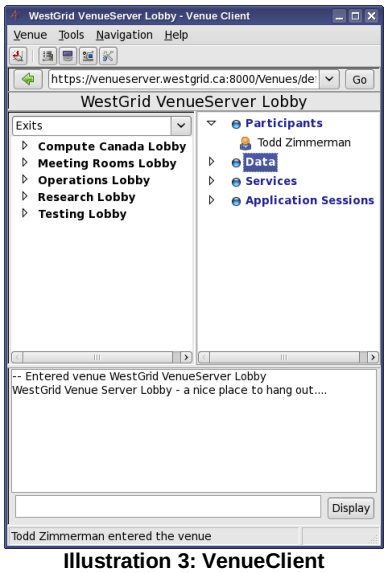

Illustration 3: VenueClient

You will also see the audio (RAT) and video (VIC) applications appear. Depending on whether you are multicast enabled or not, you may or may not see other video/audio streams in those applications.

Checking Multicast Connectivity - Using the Multicast/Unicast Bridge

You can determine your multicast connectivity status by looking at the icon in the upper left of the VenueClient (below the 'Venue' toolbar entry). By hovering over the Multicast Connectivity icon, your connectivity status will be displayed.

If your do not have mutlicast connectivity, you will have to use a Multicast to Unicast bridge to communicate with other AG participants.

To access the bridge:

1. **Select Tools -> Bridges -> WestGrid from the VenueClient toolbar**

If you want to permanently use the WestGrid bridge so that you don't have to select it every time you start:

To permanently use the WestGrid bridge:

1. **Select Tools -> Preferences from the VenueClient toolbar**
2. **Select the Bridging section on the left**
3. **Select 'Always use unicast bridges....' at the top**
4. **Uncheck 'Measure closeness to bridges...' in the Bridges section**
5. **Use the 'Move Up' button to ensure the WestGrid bridge is listed at the top of the list of bridges.**

Adding Video Capture Capability

By default, AccessGrid nodes will receive and display all remote site video feeds; however, it will not send video from your local camera to the remote sites without first changing your Node Service configuration.
Detailed instructions on Adding Services can be found in the 'Adding a Service to a ServiceManager' section below; however, here are quick instructions for changing your 'receive only' video service to also send your local video.

To send your video to remote sites:

1. **Select 'Tools' -> 'Configure Node Services' from the VenueClient menu**
2. **Right click the 'Video Consumer Service' and choose 'Delete'**
3. **From the menu, select 'Add...'**
4. **From the pop up, select 'VideoService'**
5. **Select the appropriate capture resource**
6. **From the menu, select 'File' -> 'Store Configuration'**
7. **In the save dialog, enter a new name for your configuration, and check the 'Set as default' checkbox**

Basic Video (VIC) Operation

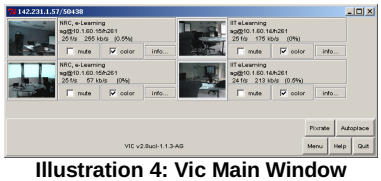

Illustration 4: Vic Main Window

Vic's main window shows all of the available video feeds as thumbnails. The number of columns of thumbnails that are displayed can be changed by pressing the number key (1,2,3, or 4) associated with the desired number of columns. The image to the right shows the main page with a column width of two wide.

By clicking the mouse on the thumbnails, the individual video feed will enlarge to become its own window – available to be placed and sized independently, as shown to the left. The size of the individual video feed window can be changed by pressing s, m or l (small, medium or large). For feeds with a "frame" the frame can be cut using shift-s, shift-m and shift-l.

Illustration 5: Vic Single Video

By selecting the "menu" button on Vic's main page, the capture device can be selected by choosing the "Device" button – and the "Transmit" checkbox can be (de)selected depending on whether you would like to transmit video. Also, the quality of the video transmission can be adjusted based on current network conditions or personal preferences.

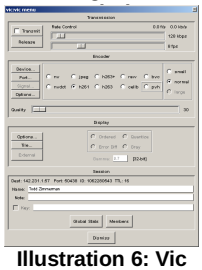

Illustration 6: Vic Options

Basic Audio (RAT) Operation

The rat interface offers the ability to control all reception and transmission options for the audio component of the collaboration. To transmit audio, make sure the "Talk" checkbox is checked – and the appropriate input (microphone or line-in) is selected below the talk button (Line-In is chosen in the image). You can scroll through available inputs by clicking on the arrow keys beside the selected input – below the talk button.

The slider under the level meter will adjust the input level. To change any personal information or settings, press the "Options" button.

Beside each participants name is a slider which can be used to adjust individual volumes for specific participants.

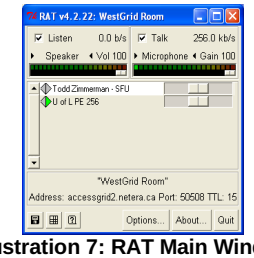

Illustration 7: RAT Main Window

For more information on operating VIC, visit the UCL Multimedia website located at http://www-mice.cs.ucl.ac.uk/multimedia/software/vic/index.html *Also, you can find a helpful user's guide located at* http://www.vrvs.org/Documentation/Applications/vic-userguide.pdf

Rat uses sockets to communicate between the main application and the gui. If you have a personal firewall running on your AccessGrid node, the GUI may be blocked from appearing. To alleviate this problems, allow UDP port 47000 from your own IP address through the firewall.

VenueServer Navigation

The AG uses a venue, or room, based metaphor for organizing collaborative sessions. Venues are linked by doors, which allow users to navigate from one venue to another. The collaborative media (audio, video, shared applications) that are associated with a given venue are scoped by the venues themselves. That is, as you move from venue to venue, the collaboration tools are automatically reconfigured to connect to other users in that venue. No action on the part of the user is required.

The WestGrid venue server provides a set of venues for WestGrid related research groups to meet. A number of casual meeting venues have been created for WestGrid researchers to gather. The main WestGrid Lobby is the highest level general meeting place. Other venues have been created such as an Operations Lobby, a Research Lobby, a Meeting Rooms Lobby and a Compute Canada Lobby. These venues are intended as casual meeting places as well, with the Operations Lobby a meeting place with an operational focus (site administration, steering committees, etc.) and the Research Lobby a meeting place with a research focus. Off of each of these lobbies a set of meeting venues will be constructed as required by the appropriate groups. A typical venue in the Operations Lobby would be a meeting room for the Site Leads. A typical venue in the Research Lobby would be a meeting venue for a specific project. To create a venue for a specific purpose, WestGrid users should contact support@westgrid.ca for assistance.

The video and audio conferencing for the AG venues are handled by separate programs – VIC for video, and RAT for audio. Once you have successfully connected to a VenueServer, both the VIC and RAT applications should launch in separate windows. See the 'Basic VIC Operation' and 'Basic RAT Operation' sections Adding a Service to a ServiceManagerbelow for more information on the audio and video settings.

To navigate to other rooms:

1. Click on the selected venue on the left

In a few seconds, all of the tools and services will restart, and you will now be located in the new room.

To text chat with other participants, enter your text in the text area labeled 'Your Message' and press Enter or press the 'Display' button.

Node Management – Services and ServiceManagers

AG VenueClients use ServiceManagers to manage services when connecting to venues. In fact, a single VenueClient can control multiple computers – each running a ServiceManager to create a room based node.

On each machine that is part of an AccessGrid node, a ServiceManager must be running. Each ServiceManager controls the particular services (video/audio) running on that particular machine. For example, in some cases AccessGrid nodes consist of two computers - one computer to handle all of the capture (audio and video), and a second computer to handle all of the display output. In this case, each computer would run its own ServiceManager, and the VenueClient would connect to each ServiceManager to control the services themselves.

For an Access Grid Station, there is only one computer – so the VenueClient only connects with its own ServiceManager. While the ServiceManager is actually a completely different process from the VenueClient, the ServiceManager is started automatically when the VenueClient is launched from the desktop shortcut that was created during installation, or when it is launched from the command line with the '--personalNode ' option added.

Services provide a specific aspect of collaboration – such as audio conferencing, video display, or video capture. These services are called the AudioService, VideoConsumerService, VideoProducerService and VideoService respectively. Here is a description of the uses and capabilities of each of these services.

AudioService

The AudioService handles all of the incoming and outgoing audio configuration.

VideoService

The VideoService will handle all incoming and outgoing (capture) requirements in a single service. This is best used on a single machine node with a single capture device, such as a PIG node.

VideoConsumer

The VideoConsumerService will handle all incoming video. This service is best used on a multimachine node, for when your video display computer is different than your video capture computer.

VideoProducer

The VideoProducerService will handle outgoing video capture. You will need as many VideoProducerServices running as you have capture devices. For example, if you have 3 capture cards, you will required 3 VideoProducerServices running to manage them.

Viewing and Managing Services and ServiceManagers

To view/manage your Services and ServiceManagers:

1. **Click on Preferences -> Manage My Node**
2. **Select the 'localhost' ServiceManager by clicking on it**
3. **All of the associated services that are managed by that ServiceManager should appear in the right hand window**
4. **To change the settings of a particular service – or to delete a service, right click that service and select the appropriate function**

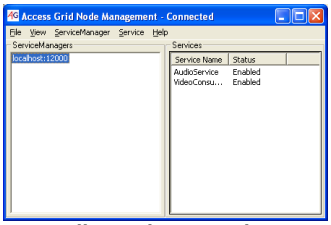

Illustration 8: Node Management Window

Adding a ServiceManager

To add additional servicemanagers (running on separate computers):

1. **Click on Preferences -> Manage My Node**
2. **From the menubar, choose ServiceManager -> Add...**
3. **In the 'Hostname' textbox, enter the hostname or IP address of the servicemanager machine. The default port for servicemanagers is 12000**
4. **Click OK**

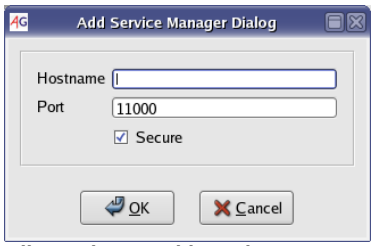

Illustration 9: Add ServiceManager Dialog

You should now see the new ServiceManager listed in the left hand window of the Node Configuration window.

Adding a Service to a ServiceManager

To or a add a service to an existing servicemanager:

1. **Select Preferences - > Manage My Node...**
2. **Single click the servicemanager you would like to add the service to**
3. **Select Service -> Add from the menubar**
4. **Select the service you would like to add (Video, VideoProducer, VideoConsumer, AudioService, etc) from the list and press OK**

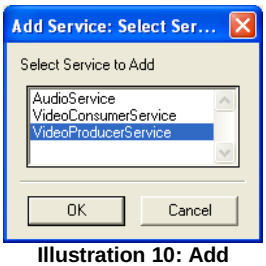

Illustration 10: Add Service Select

5. **If there are more than one devices for the service, a list of possible devices will be shown. Select the device you would like to manage.**
6. **Once added, you can properly configure your new service by right clicking the service from the right hand side of the main Node Management window.**

Saving Your Configuration

Once you have properly configured your node, you should save your settings so that you won't have to enter the same information again next time you start your VenueClient.

To save you configuration:

1. **Select File -> Store Configuration from the menubar.**
2. **Enter a name for your configuration**
3. **Check the 'set as default' check box**
4. **Press OK**

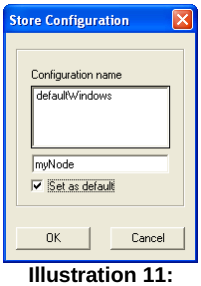

Illustration 11: Store Configuration Dialog

Certificate Management

The Access Grid software requires a valid user certificate to operate and to allow connections to external VenueServers. The first time you launch the it will automatically install an 'anonymous certificate' for your general use and no further action is typically required. This anonymous certificate should allow you to attend almost all WestGrid related AccessGrid events.

However, for some restricted events, you may need to install a proper user certificate. The section below details certificate management within the AccessGrid toolkit.

Certificates provide a means for authentication and authorization for users using the Access Grid. Each user of the AG needs to have a certificate that has been assigned to them through a recognized certificate authority. Currently the AG uses certificates from the Argonne National Lab. Within the WestGrid AG community, it is also possible to use Grid Canada certificates to access the AG infrastructure. See the "Using Grid Canada Certificates" for information on how to use your existing Grid Canada certificates. If you would like to request a certificate from either Argonne or Grid Canada, see the 'Requesting a New Certificate' section for more details.

Certificates are authenticated using a user entered 'Passphrase'. This user enters this passphrase to securely and uniquely identify themselves as the owners of the certificate.

During AG use, AG users create a proxy (which is valid for a fixed amount of time) based on their certificate. This proxy allows them to access resources within the Grid infrastructure. In the AG context, users are asked for their certificate passphrase to create a proxy if a proxy for that user is not currently valid. Once the proxy is created, users can use the VenueClient to navigate from meeting venue to meeting venue without having to authenticate.

To manage certificates for the VenueClient:

1. **Click on Preferences -> Certificate Manager...**
2. **Choose your Certificate Management activity.**

Some of the activities include - Importing or Viewing your Identity Certificates, Importing or Viewing your Trusted CA Certificates, Importing the Default Globus Certificates, Requesting a Certificate or Viewing Pending Requests.

Importing Certificates

To import an existing certificate into the VenueClient, the certificate and key files should be in .pem format. This is the format that they should be provided in when they are issued to you by the certificate authority.

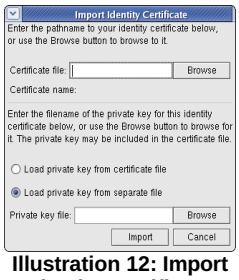
Import Identity Certificate
Enter the pathname to your identity certificate below, or use the Browse button to browse to it.
Certificate file:
Browse
Certificate name:
Enter the filename of the private key for this identity certificate below, or use the Browse button to browse for it. The private key may be included in the certificate file.
Load private key from certificate file
Load private key from separate file
Private key file:
Browse
Import
Cancel

Illustration 12: Import Identity Certificate

To Import A Certificate:

1. **Choose Preferences -> Certificate Manager...**
2. **Select "Import Certificate"**
3. **Browser for the appropriate certificate and key**
4. **Press Import**

You will be prompted for the passphrase of the certificate to complete the import process!

If the import was successful, you will receive a pop up message indicating success. If the import was unsuccessful, try to import the certificates again.

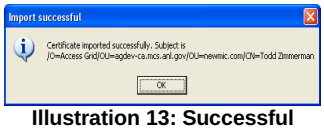

Illustration 13: Successful Certificate Import

Exporting Certificates

It is a good idea to have a backup of your certificates stored in a safe – and secure – location.

To export your certificates for backup:

1. **Choose Preferences -> Certificate Manager...**
2. **Click on the certificate you would like to export and click 'Export...'**
3. **Choose to write the certificate and key to separate files or to a single file.**
4. **Enter the preferred location and name of the new certificate and/or key files.**
5. **Press 'Export Certificate'**

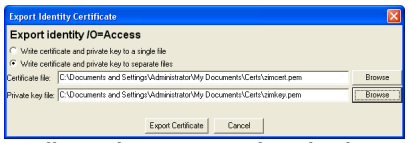

Illustration 14: Exporting Identity Certificates

If the export process was successful, you should be able to copy/import the files as required.

Requesting A New Certificate

To Request A Certificate:

1. **Open the Certificate Management window by selecting "Preferences -> Request a Certificate"**
2. **Click 'Next' to continue with the Certificate Request process**
3. **Select the type of certificate you would like to request (Identify (personal certificate), anonymous, or service (machine).**
4. **Press Finish to complete the request.**

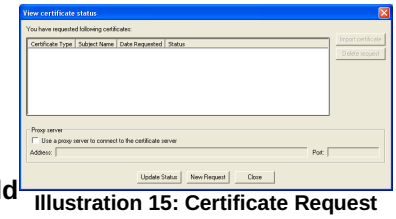

Illustration 15: Certificate Request Status

A Certificate Request will automatically be sent to Argonne National Labs to be approved.

You will have to wait until ANL responds to your certificate – see Viewing/Importing Pending Requests below.

Viewing/Importing Pending Requests

To Monitor Your Pending Certificate Requests:

1. **Clicking on Preferences -> Certificate Manager...**
2. **Click on the Certificate Requests tab**
3. **Locate you request and check the 'Status' field. You can also refresh the status by choosing the 'Check Status' button**
4. **If your certificate is ready, you can then select the certificate – and choose "Import" to integrate your certificate into the VenueClient.**

Using Grid Canada Certificates

The WestGrid community uses the Grid Canada certificate authority for user authentication. When a person applies for a WestGrid computing account from www.westgrid.ca, that person automatically receives a Grid Canada certificate. The certificate can be found in the user's home directory under a directory called '.globus'. Within that directory are the user's public certificate and the user's private key files (usually usercert.pem and userkey.pem). These certificates can be used to within the WestGrid AG infrastructure.

The first step to using the Grid Canada certificate authority is to import the Grid Canada 'root certificate' and 'signing policy' files. These files give your AccessGrid station the ability to authenticate Grid Canada certificates.

To import the Grid Canada root certificate and signing policy:

1. **Download the required files from http://www.gridcanada.ca/ca/index.html . The files required are the 'GC CA Certificate' (bffbd7d0.0) and the 'GC CA Certificate Signing Policy' (bffbd7d0.signing_policy)**
2. **In your AccessGrid VenueClient, choose Preferences->Certificate Manager...**
3. **Click on the 'Trusted CA Certificates' tab, and choose 'Import'**
4. **From the 'Open File' dialog box, navigate to the newly downloaded bffbd7d0.0 Certificate file and press 'Open' The signing_policy file will probably automatically be found. If not, navigate to the newly downloaded bffbd7d0.signing_policy file and press 'Open'**

The certificate should now be successfully imported!

If you don't receive a 'Certificate imported successfully' dialog box - contact support@westgrid.ca for more help.

The next step to using Grid Canada certificates is to import your individual user certificate and key.

To import your certificate:

1. **Locate your personal certificate and key file from WestGrid computing. The files are usually located in your ~/.globus directory (usercert.pem and userkey.pem).**
2. **Copy the files to a known location on your local computer.**
3. **From the AG VenueClient, choose Preferences -> Manage Certificates -> Certificate Manager...**
4. **Click the Certificates tab and choose "Import"**
5. **From the Dialog box, select the certificate and key files that you just copied and press 'Open'.**
6. **Enter the passphrase for the certificate so that authenticity can be checked.**

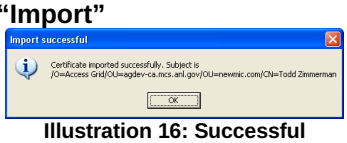

Illustration 16: Successful Certificate Import

If the import was successful, you will receive a pop up message indicating success. If the import was unsuccessful, try to import the certificates again.

If you don't receive a 'Certificate imported successfully' dialog box - contact support@westgrid.ca for more help.

Now, you should be able to use your Grid Canada certificates. The final step is to set your new Grid Canada certificate as your 'default' certificate.

To Set A Default Certificate:

1. **Choose Preferences->Manage Certificates-> Certificate Manager...**
2. **Click the Certificates tab**
3. **Select your newly imported Grid Canada certificate**
4. **Click the 'Set as Default' button**
5. **Restart your VenueClient software**

After the restart, you should be prompted to create a proxy for the new default certificate.

Remember that most VenueServers not affiliated with WestGrid do not accept Grid Canada certificates for authentication! To access other VenueServers, you will have to reset your 'default certificate' to your Argonne or anonymous certificate.

Creating A Globus Proxy

If you are not running an anonymous certificate, you may be prompted to 'Create a Globus Proxy'.

A proxy is used to temporarily authenticate you to the AccessGrid. The length of time the proxy is valid for can be adjusted when you are prompted to create it. Typically, proxy's last 8 hours.

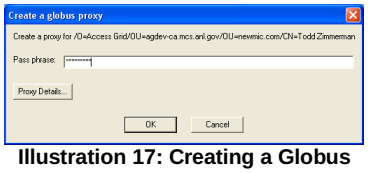

Illustration 17: Creating a Globus Proxy

To Create A Globus Proxy:

1. **Click on 'Proxy Details' to change the length of time the proxy will be valid for**
2. **Enter your certificate passphrase**
3. **Press 'OK'**

Additional Resources

The main WestGrid Access Grid webpage has many helpful documents that may be of assistance to you. Also, many additional resources and help files can be found on the Internet by searching Access Grid, or by visiting the main Access Grid site at http://www.accessgrid.org

Links

Some specific links to helpful information:

WestGrid Access Grid Documentation

All of the documentation required to use the AccessGrid on the WestGrid network. http://www.westgrid.ca/support/collaboration

Access Grid Documentation

One of the main sites for accessgrid information.
http://www.accessgrid.org/documentation/

The Access Grid Documentation Project

Another great site for detailed instructions and helpful guidence.
http://www.accessgrid.org/agdp/

Vic User Guide

A very detailed userguide for Vic – the AccessGrid's video application used for capturing and receiving video streams.

http://www.vrvs.org/Documentation/Applications/vic-userguide.pdf

AccessGrid Mailing Lists

There is also some great information which can be found in the various AG mailing lists – most are archived and searchable at www.accessgrid.com

Troubleshooting

Network

Most network issues are a result of a failure of multicast. These issues can be hard to diagnose and even harder to fix due to the fact that many times, the problem doesn't exist on your network segment.

You can help troubleshoot the network problems by installing Internet2 detective (http://detective.internet2.edu/)

You can also check general multicast connectivity by visiting the "Multicast Beacon" site at http://beacon.dast.nlanr.net/ .

To fully utilize the beacon, the beacon software would also need to be installed. Visit http://dast.nlanr.net/Projects/Beacon/ for more information.

Video

Video tends to be one of the easier aspects of the AG to set up; however, there are a couple of 'gotchas' to be aware of.

Reception Greyed Out

If you are receiving video feeds, but all of them are 'greyed out', you have set up a 'Video Producer' instead of a 'Video Consumer'. If you would like to view video feeds from other sites – add a Video Consumer service to your node.

No Feeds Received

If you are not receiving any feeds - but are sure that there are feeds being sent from other sites, make sure that your multicast is working correctly. Try using the unicast bridge to see if the problem is resolved.

Vic Crashes

If the video transmit options are incorrectly set – VIC can unexpectedly crash. To solve VIC crashes on startup/transmit, click on the "menu" button on Vic's main page, and choose Options->Configure on Transmit. Then, click on the transmit button to begin video capture. A transmit configuration box should appear. On this configuration screen – be sure to select a resolution that AG Vic can handle – no higher than CIF (352x288).

Selecting a Video Source

Depending on what kind of capture card / webcam device you are using, the 'Device...' selection may show up in different ways. If your specific device shows up in the 'Device Selection' dialog, that is the preferable selection. If your specific device is not listed, the default capture device that can be used for webcams in Windows is 'Microsoft WDM Image Capture (Win32)'.

Audio

So much of the quality of a video conference can be attributed to audio quality that a lot of time is spent making sure that the audio subsystem is working adequately. When audio issues arise, they can often be fatal to a meeting or collaboration – so having a backup plan (such as a telephone) is always a good idea.

These audio issues can sometimes be hard to diagnose; however, by logically following the path of the sound, the problem can usually be found. As with any computer problem, rule number one with all audio issues is to check (and double check) the wiring/cabling. Many issues can be solved by checking to make sure everything is plugged in properly.

Reception

If you are having a problem with reception, first try to diagnose if it is a single site or all sites that you are having issues with.

If it is a single site – it may not be your issue at all. Ask some other participating sites if they are also experiencing the problem and try to diagnose it.

If the issue is consistent over all of the sites, then you will need to try to narrow down the possible causes. If you aren't receiving *any* audio, try some of the following:

- Make sure the "Listen" checkbox is selected on the main RAT window
- Double click the "Volume" icon in the system tray and be sure the "Volume Control" is at an appropriate level and "Mute All" isn't selected.
- Double click the "Volume" icon in the system tray and be sure the "Wave" level is also appropriately set – and not muted.
- **If you are using an "onboard" Intel sound card, a number of users have experienced conflicts with the RAT software.**

If you are receiving audio, but the quality is low, try playing a CD or other media file to see if the problem is RAT specific.

Transmission

If you are having a problem with transmitting audio, try the following:

- Make sure the "Talk" checkbox is checked in Rat
- Make sure the microphone cable is plugged into the Microphone input of your computer/sound card (usually it is RED). If your computer doesn't have a Microphone input – you can use the "Line In" input (usually BLUE).
- Make sure that the appropriate input source is selected below the "Talk" checkbox in Rat (Usually "Line In" or "Microphone")
- Double click the "Volume" icon in the system tray, select Options then Properties. In the window that pops up, select Adjust Volume For: "Recording" and be sure the input that your microphone is plugged into is checked in the "Show the following volume controls" list below. Then select OK.

- A new window will appear containing the "Recording" levels and controls. On this window, be sure that the "Select" checkbox for whichever input you are using is selected – and be sure that the level is around 70 – 75%.
- If you can hear yourself in your headphones, double click the "Volume" icon in the system tray, and be sure that the Mute checkbox for the input source (usually Microphone) is checked. If you do not see a slider for your input source – you can click on Options, choose Properties and select which volume controls to view from the checklist.

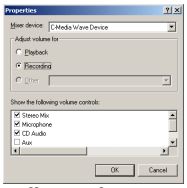

Illustration 18: Windows Recording Select

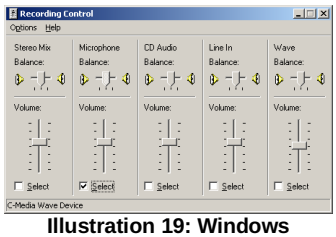

Illustration 19: Windows Recording Volume Control

Contact

For more information about the Access Grid and WestGrid – or if you have any questions about this document, please contact WestGrid AG Help at support@westgrid.ca